Presentation Title: The Structure of Groups

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Md. Mehedi Hasan
IT-23606
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

① Ans. Quantum computing poses a significant threat to traditional cryptographic protocols, particularly public-key crypto systems like RSA and ECC. The primary algorithm shors which can efficiently factor large-integers and solve the discreate algorithm problem in polynomial time.

The implication includes:-

i. loss of confidentiality
ii. compromised integrity
iii. Long term security risk.

Post Quantum Cryptographic Algorithms:- To counter the quantum threat, researches are developing post-quantum cryptography algorithms that are resistant to quantum attacks.

1. Lattice based cryptography:

→ Algorithms: crystal kyber
→ Resistance: The security is based on hard lattice problems such as the learning with errors problems.
→ Strengths: Efficient operations and well understood security foundations.

2. code based cryptography:

→ Algorithm: classic mcEliece.
→ Resistance: Based on the difficulty of random linear codes.

IT-23606

3. Hash-based cryptography:

-> Algorithm: stateless hash based signature.

-> Resistance: Based on the security of cryptographic hash functions are resistant to quantum attacks.

-> strength: stateless design ensures security without requiring state tracking.

for instance:

-> Lattice problems remain hard even with quantum speed

-> code based cryptograph relies on an error-correcting problem that quantum computers cannot solve efficiently.

(2) Ans: Implementation:-

```
import time
import os
class customPRNG:
    def __init__(self, seed = None, mod = 100):
        if seed is None:
            self.seed = int(time.time()*1000000)^os.getpi
        else:
            self.seed = seed
            self.mod = mod
        def next(self):
            self.seed ^= (self.seed << 13) & 0xFFFFFFFFFF
            self.seed ^= (self.seed >> 7) & 0xFFFFFFFFFF
            self.seed ^= (self.seed << 17) & 0xFFFFFFFFFF
            return abs(self.seed) % self.mod
```

```
def random_list (self, size):
    return [self.next() for _ in range(size)]

# Example usage:
prng = custom_prng(mod = 1000)
print(prng.next())
print(prng.random_list(5))
```

③ Ans: comparison between traditional ciphers and modern symmetric ciphers:

Traditional ciphers	modern symmetric ciphers
1. Encryption speed fast.	1. fast but computationally heavier
2. Decryption speed same as encryption.	2. similar to encryption optimize for speed.
3. security weak against brute force, frequency analysis and pattern detecti	3. strong again brute force and statistical attack.

strength and weakness:

Traditional ciphers:

① Caesar ciphers:

strength: simple and easy to implement.

weakness: only 25 possible keys, vulnerable to frequency analysis.

④ Ans: Defining the action of S_4 on 2-element subsets:

The symmetric group S_4 consists of all permutations of the set $X = \{1, 2, 3, 4\}$ we define an action of S_4 on the set of 2-element subsets of X as follows:

for any $\sigma \in S_4$ and any subset $\{a, b\}$ where $a, b \in X$ and $a \neq b$ define,

$$\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$$

Proving the action is well defined:

To show that this action is well defined, we must verify,

① The image of a 2-element subset under any permutation is until a 2-element subset.

② The identity element of S_4 acts trivially.

③ The composition of two permutations become as expected.

closure: If $\{a, b\}$ is a 2-element subset of X. then for any $\sigma \in S_4$ $\sigma(a) \neq \sigma(b)$ because σ is a bijection. Hence $\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$ is still a 2-element subset.

(5)am: We are given the finite field GF(2^4) which is constructed using the irreducible polynomial

$$x^4+x+1$$

constructing GF(2^4).

Since GF(2^4) is a degree-2 extension of GF(2) we define an element as a root of the irreducible polynomial

$$\alpha^4+\alpha+1=0$$

$$\alpha^4=\alpha+1$$

since GF(2) = {0, 1} we construct the elements of GF(2^4) as:

$$GF(2^4)=\{0, 1, \alpha, \alpha+1\}$$

we know consider the non zero elements:-

$$E=\{1, \alpha, \alpha+1\}$$

① Closure: we compute the product:

$1.\alpha=\alpha.1.\ (\alpha+1)=\alpha+1$ and $1.1=1$

$\alpha(\alpha+1)=\alpha^2+\alpha=(\alpha+1)+\alpha=1$

$(\alpha+1)(\alpha+1)=\alpha^2+2\alpha+1=(\alpha+1)+2\alpha+1$

$=\alpha.\alpha=\alpha^2=\alpha+1$

Since all products remain in E ⇒ closure holds.

IT-23606

① Ans: Define the General Linear Group $GL(2,\mathbb{R})$:

The General linear group $GL(2,\mathbb{R})$ consists of all 2×2 invertible matrices over $\mathbb{R}$:

$$GL(2,\mathbb{R}) = \{ A \in M_{2\times 2}(\mathbb{R}) \mid \det(A) \neq 0 \}$$

This is a group under matrix multiplication.

Define the set of scalar matrices:-

A scalar matrix is a multiple of the identity matrix.

$$S = \{ \lambda I \mid \lambda \in \mathbb{R}^* \} = \left\{ \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid \lambda \neq 0 \right\}$$

since λI is invertible for all $\lambda \neq 0$.

constructing the factor group:

The quotient group $GL(2,\mathbb{R})$ consists of cosets of the form:

$$[A] = AS = \{ A(\lambda I) \mid \lambda \neq 0 \}$$

since λI scales all the element uniformly. two matrices A and B belong to the same coset if and only if they differ by a scalar multiple:

$$A \sim B \iff B = \lambda A \text{ for some } \lambda \neq 0$$

This means that the cosets represent equivalence classes of matrices under

IT-23606

(7) Ans: Difference Hellman key Exchange Protocol

The Diffie-Hellman (DH) key exchange is a cryptographic protocol that allows two parties to securely establish a shared secret over an insecure channel without directly transmitting the secret itself.

Steps of the Protocol:-

1. public Parameters selection.
2. key exchange btn two Parties.
3. Shared secret computation.

potential Attacks and Defenses:

1. Man in the middle attack:

Attack: An attacker intercepts messages and establishes separate key exchanges with Alice and bob

Defense: use authenticated key exchange to verify.

2. Brute force on pre computation Attacks:

Attack: If the Prime p is small an attacker can precompute logarithms for all value.

Defense: use large primes to prevent of such attack

JT-23606

(8) Ans: Proof: Let G be a group and let H and K be two subgroups of G. We want to show that the intersection $H \cap K$ is also a subgroup

Step1: Show $H \cap K$ is non-empty since H and K are subgroups, they both contain the identity element e of G $e \in H$ and $e \in K$

Step 2: closure under multiplication:

Let $a, b \in H \cap K$

since both H and K are subgroups, they are closed under multiplication, so.

$ab \in H$ and $ab \in K$

Thus $ab \in H \cap K$ proving closure under multiplicat

example:

consider the group of integers under addition

$G = Z$ and let

$H = 2Z = \{\ldots -4, -2, 0, 2, 4 \ldots\}$

$K = 3Z = \{\ldots -6, -3, 0, 3, 6 \ldots\}$

The intersection $H \cap K$ consists of all integers that are both even and divisible 3 and 6

$H \cap K = 6Z = \{\ldots -12, -6, 0, 6, 12 \ldots\}$

$6Z$ is a valid subgroup of Z.

IT-23606

(10) Ans: Vulnerable of the DES cipher:-

The Data Encypher standard developed in the 1970s was one of the most widely used symmetric encrypt algorithms. How ever due to advancement in compu power and analysis. DES is now considered insecur for modern application.

① short key length.
② Brute force attack
③ cryptanalytic weakness
④ small block size.

Brute force Attack Break DES:-

A brute force attack ~~break~~ systematically tries all possible keys until the correct is found
→ with 56-bit key there are $2^{56} \approx 72 \times 10^{-15}$ possible keys.

→ modern hardware, such as ASICs, FPGAs, and cloud based Parallel processing can exhusted this key

AES Addressed the short coming DES:

The Advanced Encryption standard (DES) was introduced in 2001 to replace DES and overcome is weakness.
→ Increased the key size.
→ Large block size.

IT-23606

(14) Ans; Differential cryptanalysis is a chosen plain text attack that analyze how difference in plaintext propagate through a cipher to predict differences in ciphertext.

Defense mechanisms in DES Against DC:-

1. S-Box Design to resist DC:

The s-boxes in DES were carefully designe to minimize differential probabilities

2 Reistal structure Provides:

In this Reistal network of DES, the right half of the block is expanded, mixed with the round key,

ii) Unlike DES, AES is not a Feistal cipher but follows a substitution-permutation structure to DC.

key features that improve DC resistance:

i) substitutes
ii) shiftrows
iii) mix column for strong Diffusion.
iv) Add round key
-) more round in AES on AES-128 has 10 rounds.

IT-23606

(12) Ans: Finding the modular inverse using the extended Euclidean algorithm:-

The modular inverse of an integer modulo n is an integer x such that;

$$a \cdot x \equiv 1 \pmod{n}$$

This means that x is the multiplicative inverse of a modulo n, provided that a and n are coprime ($\gcd(a,n)=1$). we use the extended Euclidean algorithm.

step1: Apply the euclidean algorithm. The algorithm finds the greatest common divisor (gcd) of a and n using the divison algorithm.

$\gcd(a,n) = \gcd(n, a \bmod n)$

we continue until we reach $\gcd = 1$

step2: Apply the extended euclidean algorithm: The EEA express $\gcd(a,n)$ as a linear combination.

$\gcd(a,n) = ax + ay$

Since $\gcd(a,n) = 1$ we can rewrite this as

$$1 = ax + ay$$

reducing modulo n

$$ax = 1 \pmod{n}$$

Thus x is the modular inverse of a modulo n.

IT-23606

(3) Ans; ECB mode is insecure for highly redundant data:-

In electronic codebook (ECB) a plain message P is divided into fixed size block and each block is independently encrypt using the same key K

$$C_i = E_K(P_i)$$

mathematical Proof of ECB weakness:-

1. Lack of Diffusion; Indentical plaintext blocks Produce identical ciphertext blocks.

suppose we have two plaintext block P_i and P_i such that

$$P_i = P_i$$

since encryption in ECB is deterministic

$$C_i = E_K(P_i) = E_K(P_i) = C_i$$

This means that identical plaintext blocks always produce indentical ciphertext block which leaks information about the structure of the plain text.

IT-23606

(14) Ans: A linear feedback shift register generates a repeating sequence of bits using a linear formula.

$$S_n = e_1 S_{n-1} \oplus e_2 S_{n-2} \oplus \dots \oplus e_m S_{n-m}$$

where → S_n are the output bits
→ e_i are fixed numbers
→ $\oplus$ is XOR

This linear means an attacker can set up simple equations and solve them to find the LFSRs structure

A hacker Breaks LFSR encryption:-

A stream cipher using a LFSR encrypt data like this, $c_i = p_i \oplus K_i$

p_i = plaintext

K_i = LFSR generated key stream bit

If a hacker know that both p_i and c_i they can recover k_i,

$k_i = c_i \oplus p_i$

Since the key stream follows a linear. the hacker can use math tricks to find all future k_i. This break the encryption.

IT- 23606

(15) Ans: Claude Shannon defined Perfect Secrecy mathematically as

$$P(m|c) = P(m)$$

for all plaintext m and ciphertext c, where
→ $P(m)$ is the probability of choosing as plaintext m.
→ $P(m|c)$ is the probability of m given that we observe c

This means that knowing the ciphertext gives no additional information about the plaintext.

Using Bayes theorem, we can rewrite the condition as: $P(c|m) = P(c)$

The OTP satisfies shanons definition:-

We need to prove that knowing c does not reveal any information about M.

1. Since K is chosen uniformly at random, for any given plaintext m, the ciphertext is $c = m \oplus K$
2. The key is equally likely to be any value in K and since $|K| = |M|$ every plaintext has an equal chance of producing any ciphertext.
3. Thus key is equally likely to be any value in and since $|K| = |M|$ every plaintext has an equal chance of producing any ciphertext.

IT-23606

(16) Ans: Lets choose specific values for the LCG parameter:-

- multiplier $a = 5$
- Increment $c = 3$
- modulus $m = 16$
- seed $x_0 = 7$

The recurrence relation is $x_{n+1} = (a x_n + c) \bmod m$

substituting our values:

$$x_{n+1} = (5x_n + 3) \bmod 16$$

Now, we compute the first 5 values:-

1. $x_1 = (5 \times 7 + 3) \bmod 16 = (35+3) \bmod 16 = 38 \bmod 16 = 6$
2. $x_2 = (5 \times 6 + 3) \bmod 16 = (30+3) \bmod 16 = 33 \bmod 16 = 1$
3. $x_3 = (5 \times 1 + 3) \bmod 16 = (5+3) \bmod 16 = 8 \bmod 16 = 8$
4. $x_4 = (5 \times 8 + 3) \bmod 16 = (40+3) \bmod 16 = 43 \bmod 16 = 11$
5. $x_5 = (5 \times 11 + 3) \bmod 16 = (55+3) \bmod 16 = 58 \bmod 16 = 10$

The sequence is 6, 1, 8, 11, 10

IT-23606

(17) Ans:- A ring is a set with two operations, additions and multiplication that follow certain rules. Rings are algebraic structures that generalize fields.

These operations must satisfy a few key properties,

1. Additive closure: for all $a, b \in R$, $a+b \in R$
2. Additive Associativity: for all $a, b \in R$
$(a+b)+b = a+(b+c)$
3. Additive identity: there exist an element $0 \in R$ such that $a+0=a$ for all $a \in R$
4. Additive Inverses: for each element $a \in R$ there exist an element $-a \in R$ such that $a+(-a)=0$
5. multiplicative closure: for all $a, b \in R$, $a.b \in R$
6. multiplicative Associativity: for all $a, b, c \in R$
$(a.b).c = a.(b.c)$
7. Distributivity of multiplication over addition: for all $a, b, c \in R$ the multiplication distributes over addition:
$a.(b+c) = (a.b)+(a.c)$
$(a+b).c = (a.c)+(b.c)$

TT-23606

(18) Ans: (i) Given $p = 5, q = 11$

compute $n = p.q = 5.11 = 55$

$\phi(n) = \phi(p).(q-1) = 4.10 = 40$

choose $e = 3$ where $\gcd(3, 40) = 2$

compute d such that,

$e.d = 1 \pmod{40}$ and $d < 40$

value is $d = 27$ since $3 \times 27 = 81 = 2 \times 40 + 1$.

The public key is $(e, n) = (3, 55)$

The private key $(d, n) = (27, 55)$

Let the message $m = 2$

Encryption:

ciphertext $c = m^e \bmod n$

$= 2^3 \bmod 55$

$c = 8$

Decryption

using the decription formula:-

$m = c^d \bmod n$

$= 8^{27} \bmod 55$

message = 2

IT-23606

(19) Ans: We are given the elliptic curve equations:-

$$y^2 = x^3 + ax + b \bmod p$$

with parameters:-

$p = 23,\ a = 1,\ b = 1$

i) Verify if $P = (3, 10)$ on the curve. To check if the point $P = (3, 10)$ lies on the curve, substitute $x = 3,\ y = 10$ into the equations,

$$10^2 = 3^3 + 1(3) + 1 \bmod 23$$

$$100 = 27 + 3 + 1 \bmod 23$$

$$100 = 31 \bmod 23$$

Since $31 \bmod 23 = 8$ and $100 \bmod 23 = 8$.

both sides are equal. Thus P lies on the curve

ii) Doubling the point P:-

The formula $\lambda = \dfrac{3x_1^2 + a}{2y_1} \bmod p$

$$x_2 = \lambda^2 - 2y_1 \bmod p$$

$$y_2 = \lambda(x_1 - x_2) - y_1 \bmod p$$

substituting, $P = (3, 10)$

$$\lambda = \frac{3(3^2) + 1}{2(10)} \bmod 23$$

$$= \frac{28}{20} \bmod 23$$

$$x_2 = \lambda^2 - 2x_1 \bmod 23$$

$$= 12^2 - 2(3) \bmod 23$$

$$= 138 \bmod 23 = 20$$

IT-23606

(20) Ans:- The curve equation is: $y^2 = x^3 + 7x + 10 \bmod 37$

$G = (2, 5)$, $n = 17$, $d = 7$, $k = 3$, $1 + (n) = 8$

Step 1: compute the public key $\theta = dG$

since the public key is obtained by scalar multiplication of the best point

$$\theta = d \cdot G = 7 \cdot (2, 5)$$

we compute $9G$ using double and add

compute $2G$ (Point doubling)

formula: $\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$

$$x_2 = \lambda^2 - 2x_1 \bmod p$$

$$y_2 = \lambda (x_1 - x_2) - y_1 \bmod p$$

for $G = (2, 5)$, we have

$$\lambda = \frac{12}{10} \bmod 37$$

we compute the modular inverse of $10 \bmod 37$

$$10^{-1} = 26 \bmod 37$$

$$\lambda = 12 \times 26 \bmod 37$$

$$= 924 - 481 = 13$$

$$x_2 = 13^2 - (2) \bmod 37 = 17$$

$$y_2 = 22$$

$\therefore 2G = (17, 22)$

IT-23606

(22) Ans: A Galois field (GF(p)) is a finite set of elements where arithmatic operations are defined,

Types of Galois fields:-

1. GF(p) Prime fields:-
   - element: {0,1,2 ... p-1} where p is prime
   - used in Elliptic curve cryptography for secure encryption digital signatures and key exchange.
2. GF(2^n) (Binary fields):-
   - Elements are binary polynomials modulo an irreducible polynomial.
   - Used in AES encryption, error correction and Post quantum cryptography.

Importance is cryptography:

Efficient computation: fast arithmatic infinite fields improves performance
security: Provides resistance to attack like discreate logarithm problems.
- compact presentation:- useful for hardware and embeded system.
- mathematical Rigar:- Ensure cryptographic algorithms function correctly.

JJ-23606

(23) Ans: The shortest vector Problem (SVP) is fundamental hard problem in lattice based cryptography Given a lattice, the SVP asks for the shortest non zero vector in the lattice under a chosen form. The problem is computationally hard meaning even the best known algorithms require exponential time for large lattices.

Role in security:-

→ many lattice based cryptographic schemes rely on the difficulty of approximately SVP.

→ learning with error and Ring LWE key problem in lattice cryptographic are reducible to SVP.

→ even quantum computers are not known to solve SVP efficiently, making lattice based cryptography post quantum secure.

ii) cryptographic scheme	security basis	vulnerability to shors algorithm
RSA	Integer factorization problem	Broken by shors algorithm
Elliptic curve cryptography	Elliptic curve discreate log problem.	Broken by shors algorithm
lattice based cryptography	Lattice Problem	not efficiently solveable by quantum algorithms

(24) Ans: Step 1:

→ A linear shift feedback register is defined by the recurrence relation.

$$k_t = c_1 k_{t-1} \oplus c_2 k_{t-2} \cdots \oplus c_m k_{t-m}$$

Where,

→ the co-efficient $c_1, c_2 \ldots c_m$ belong to GF(2)

→ The operations are performed modulo 2

→ The sequence of key stream bits $\{k_t\}$ is periodic meaning it eventually repeats.

This recurrence relation corresponds to a characteristic polynomial

$$p(x) = x^m - c_1 x^{m-1} - c_2 x^{m-2} \cdots c_m$$

Step 2: The state of an LFSR at any time is determined by the m bit sequence. Since there are m bits, the total number is 2^m. However the all zero state (00...000) is not allowed in a maximal length LFSR, since, it would produce an output stream of all zero indefinitely. Therefore the maximum possible nonzero state is

$$2^m - 1$$

Thus the maximum possible period of the key stream is $2^m - 1$.

IT-23606

(25) Ans:

An LWE based signature scheme exists of three main steps

1. Key Generation
→ Generate a private key s_k
→ compute the public key p_k using a matrix A and the LWE problem structure.

2. Signing:
→ Hash the message m to create a challenge.
→ Use the private key s_k and a trapdoor function to produce a short lattice vector.

3. verification:
→ Use the public key p_k to check.
→ If the verification equation holds, the signature is valid.

ii) Step-1:
→ choose a random matrix $A \leftarrow Z_a^{n \times m}$
→ Generate a separate key s_k
→ compute the public key.

$$p_k = A \cdot s_k + e$$

where e is a small error vector sampled from a noise distribution.